

Chapter 4

Gendered Cyber Insecurity: Between Legal Architecture and Lived Reality

Fazle Wakil, Research Scholar, Department of International Relations, Jadavpur University and

Anneshya Sanyal, Research Scholar, School of International Relations and Strategic Studies, Jadavpur University

Abstract

Cybersecurity, a foundation stone of the digital age, affects individuals across all demographics, yet its connection with gender is often unnoticed. The surge in importance of cybersecurity has not diminished the ever-present obstacles related to gender equality and the underrepresentation of women in this field. From online harassment to cyber-stalking, from cyber-bullying to hate speech, from threats to image-based abuse, from revenge pornography to discrimination, women and other marginalised genders experience heightened risk of cybersecurity. The gendered approach to cyber security is interconnected with the other aspects; complexities and needs of people based on gender, religion, race and sexual orientation. Gender-based violence is not a new phenomenon, but its migration to the digital world has magnified its scale and impact. The digital age has transformed how people interact, communicate, and conduct business. While the internet has provided numerous benefits, it has also given rise to new forms of crimes, particularly cybercrimes against women. These crimes not only invade the privacy of women but also threaten their safety, dignity, and mental well-being.

The rapid revolution in the IT industry, with a cornerstone of Artificial Intelligence, has affected the lives of individuals at large. People are more connected and engaged with each other on online platforms compared to physical interactions. These developments have assisted in some instances, but put privacy in danger. Women fear giving any of their details on any online platform due to the lack of security and privacy. Gender and cybersecurity are two correlated terms which have gained popularity in recent years. Privacy and security are still questioned in this era. Despite global progress and increased representation of women across various fields, this issue remains a major setback, limiting potential advancements in cybersecurity as a crucial societal factor. This imbalance deprives the field of talent and weakens its capacity to address new threats. In the field of cybersecurity specifically, according to figures from the International Information Systems Security Certification Consortium, that are based on a study carried out in 2019, women who work in cybersecurity represent only 24% of the total workforce globally.

Cybercrime against women has emerged as a critical concern within the United Nations system, particularly through the work of the International Telecommunication Union (ITU). Since its establishment in 1865, the ITU has addressed evolving technological risks from telegraphy to the internet age recognizing cybersecurity as foundational to a connected society. The proliferation of malware, cyber terrorism, and organized digital crime has intensified vulnerabilities,

disproportionately affecting women online. The rise of cybercrimes against women in India has also prompted the development of a multi-layered legal framework. The Information Technology Act, 2000 criminalizes hacking, identity theft, and electronic stalking, while enabling specialized cybercrime investigation cells. The Indian Penal Code has been amended to address voyeurism, cyberstalking, and non-consensual dissemination of intimate material. Additionally, the Protection of Women from Domestic Violence Act, 2005 extends protection to online harassment within abusive relationships. Although this framework is normatively robust, enforcement deficits, limited institutional capacity, and low awareness among women continue to constrain effective access to justice and meaningful digital protection.

Despite this layered statutory architecture, the paper argues that the gap between law on the books and law in action remains significant. The existence of multiple statutes and institutional mechanisms inevitably raises a critical question: have these legal interventions meaningfully reduced cybercrimes against women, or are such offences continuing to escalate in scale? The available trends suggest that reported cases are rising year after year which partly due to increased awareness and reporting, but also because digital dependence has deepened across every sphere of life. In an era where education, employment, governance, finance, and even intimate relationships are mediated through technological platforms, disengagement from digital systems is neither feasible nor desirable. This structural dependence renders women simultaneously visible, accessible, and vulnerable in unprecedented ways. Also while dealing against cybercrime as a whole, the inquiry must move beyond statutory adequacy to assess whether institutions possess technological capacity, trained personnel, and gender-sensitive protocols, while critically examining accountability when violations arise externally or within power structures, complicating the assumption of the state as an unequivocal protective actor.

This paper thus moves beyond formal legal analysis to examine patterns of incidence, enforcement capacity, infrastructural preparedness, and systemic accountability. By situating cybercrime within broader structures of digital governance and gendered power relations, it seeks to evaluate whether women's digital safety is substantively secured or remains an aspirational promise within an increasingly technologized society. Finally, the paper evaluates the effectiveness of existing cybersecurity frameworks themselves. Cybersecurity often operates reactively rather than preemptively, and rapid technological innovation frequently outpaces regulatory adaptation. The study therefore assesses whether current cybersecurity mechanisms function as meaningful deterrents or merely as post-facto response systems.

Keywords: *Privacy, Information Technology Act, Gendered Cyber Violence, Digital Governance, Institutional Capacity, Women's Online Safety, International Telecommunication Union*

Introduction – Gendering Cybersecurity

The expansion of the internet and digital technologies has fundamentally transformed the architecture of contemporary social life. Digital platforms now shape the way individuals communicate, access information, conduct economic activities, and participate in political and cultural processes. From education and governance to commerce and interpersonal interaction, the

digital sphere has become deeply embedded within everyday life. Within this rapidly evolving technological landscape, cybersecurity has emerged as a critical mechanism for safeguarding digital infrastructures and protecting individuals from malicious attacks, data breaches, and unauthorized access.⁸⁰ In its broadest sense, cybersecurity refers to the set of technological, legal, and institutional measures designed to protect computers, networks, servers, devices, and data from digital threats. However, while the digital revolution has generated unprecedented opportunities for connectivity and empowerment, it has also produced new vulnerabilities that affect users in unequal ways. The risks associated with cyber threats do not operate in a social vacuum. Instead, they intersect with existing structures of inequality embedded within societies. Among the groups most affected by these vulnerabilities are women, who frequently encounter disproportionate exposure to online harassment, privacy violations, and digital exploitation. Gender biases, patriarchal social norms, and structural inequalities often shape women's experiences in digital environments, making cybersecurity not only a technical issue but also a deeply social and political one.⁸¹ As the digital domain increasingly functions as a site of social interaction, economic participation, and political expression, the absence of gender-sensitive cybersecurity frameworks raise important concerns regarding safety, equality, and access.

The relationship between gender and cybersecurity has therefore gained increasing scholarly and policy attention in recent years. Digital spaces often replicate and, at times, intensify existing social hierarchies. Women's participation in online environments is frequently shaped by cultural expectations, discriminatory attitudes, and institutional limitations that influence their access to technology as well as their ability to use it safely.⁸² A gendered understanding of cybersecurity recognizes that digital threats are experienced differently across social groups. It draws attention to the ways in which vulnerabilities are influenced by intersecting identities such as gender, race, religion, sexual orientation, and socio-economic status. Consequently, addressing cybersecurity challenges requires a broader analytical lens that acknowledges how online harms disproportionately affect certain communities.⁸³

Online harassment represents one of the most visible manifestations of gendered insecurity within digital environments. As digital communication platforms expand, they have simultaneously become spaces where abusive and discriminatory behaviour can proliferate with relative anonymity. The Dart Centre for Journalism and Trauma defines online harassment as any unwanted verbal or non-verbal behaviour that occurs in digital spaces and violates the dignity of an individual by creating a hostile, degrading, or offensive environment. This definition highlights the psychological and emotional consequences of cyber abuse, demonstrating that online harassment is not merely an inconvenience but a serious violation that can affect an individual's well-being, reputation, and sense of safety.⁸⁴ Women frequently encounter a range of abusive practices in online environments, including threats, trolling, hate speech, doxxing, cyberstalking, and other

⁸⁰ Wall DS, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007)

⁸¹ Yar M and Steinmetz KF, *Cybercrime and Society* (3rd edn, Sage Publications 2019)

⁸² Kshetri N, *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan 2013)

⁸³ Singer PW and Friedman A, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014)

⁸⁴ Ibid.

forms of targeted harassment. These practices are often rooted in misogynistic attitudes that seek to intimidate or silence women who participate in public discourse. Social media platforms, online forums, and digital communication channels have increasingly become arenas where gender-based hostility manifests through coordinated attacks and derogatory commentary. For many women, navigating digital spaces involves constant negotiation between the benefits of online participation and the risks of exposure to harassment.⁸⁵

The broader context of cybercrime further underscores the significance of these challenges. Cybercrime has become a global phenomenon, affecting millions of individuals each year. Statistical estimates suggest that cybercrime occurs at an alarming frequency worldwide, with new victims emerging every few seconds. These figures illustrate the scale of the problem and highlight how deeply cyber risks have become embedded within modern societies. As the information technology sector continues to evolve particularly with the integration of artificial intelligence, machine learning, and data-driven algorithms the digital ecosystem has become increasingly complex.⁸⁶ Individuals now rely on digital platforms not only for communication but also for financial transactions, professional activities, and personal relationships. This rapid technological transformation has led to a paradoxical situation in which increased connectivity coexists with heightened vulnerability. While digital technologies enable individuals to build networks, share knowledge, and access opportunities, they also expose users to surveillance, data exploitation, and identity-related risks. Personal information shared online can be stored, analysed, and potentially misused by a range of actors, including corporations, governments, and cybercriminals. Privacy concerns have therefore become central to contemporary debates about digital governance and technological ethics.⁸⁷

The tension between technological advancement and privacy protection has long been recognized. In 1999, Scott McNealy, the then Chief Executive Officer of Sun Microsystems, famously remarked that “privacy is dead—get over it.” Although the remark was controversial, it reflected a growing recognition that digital technologies were fundamentally altering traditional notions of privacy. Over the past two decades, the proliferation of social media platforms, mobile applications, and data-driven services has intensified these concerns. The widespread collection and monetization of personal data have blurred the boundaries between public and private life, raising important questions about who controls digital information and how it is used. For women navigating digital spaces, these developments often translate into heightened anxieties about safety and personal security.⁸⁸ Many women remain cautious about sharing personal information online due to fears of harassment, identity theft, stalking, or misuse of their data. The lack of effective institutional safeguards further amplifies these concerns. In many contexts, women perceive digital platforms as environments where privacy protections are fragile and where abusive behaviour may occur with limited accountability. As a result, the digital sphere can simultaneously function as a site of empowerment and a space of vulnerability. Research increasingly indicates that women

⁸⁵ Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)

⁸⁶ Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)

⁸⁷ Brenner SW, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press 2012)

⁸⁸ Ibid.

encounter cybersecurity threats more frequently than men, particularly in the form of gender-based harassment.⁸⁹ One of the key factors contributing to this disparity is the absence of gender responsive policy frameworks within cybersecurity governance. Traditional cybersecurity approaches have primarily focused on protecting technological infrastructures such as networks, databases, and information systems. While such protection is essential, it often overlooks the human dimension of cyber threats, including the ways in which social inequalities shape digital risks.

The neglect of gender-specific concerns within cybersecurity policy is reflective of broader patterns in which issues related to privacy, safety, and bodily autonomy are marginalized within discussions of technological development. Debates about equality and justice frequently emphasize political representation or economic participation, yet the digital security of women remains insufficiently addressed.⁹⁰ In an era in which large segments of social interaction occur online, the absence of robust protections against digital harassment has significant implications for women's ability to participate freely in digital environments. Another factor that exacerbates women's vulnerability in digital spaces is the persistent digital literacy gap. Access to technological knowledge and cybersecurity awareness remains unevenly distributed across societies. In many regions, women face barriers to technological education and digital training, limiting their ability to recognize and respond to cyber threats.⁹¹ Without adequate knowledge of privacy settings, secure communication practices, or data protection strategies, users may unknowingly expose themselves to exploitation. Addressing this gap requires targeted initiatives aimed at strengthening digital literacy, particularly among women and marginalized communities.

The gender disparities evident in contemporary digital spaces are also rooted in historical developments within the technology sector itself. Contrary to common perceptions, women played an important role in the early development of computing. During the early decades of computing history, programming was often regarded as routine clerical work and was performed largely by women. In fact, computing was sometimes described as a "pink-collar profession," reflecting the significant presence of women within the field. Female programmers and mathematicians made substantial contributions to technological innovation, particularly during the mid-twentieth century. Women's participation was especially visible during the Second World War, when female codebreakers and analysts played critical roles in decoding encrypted communications and supporting military intelligence operations. Their analytical skills and technical expertise were essential to wartime cryptographic efforts.⁹² Despite these contributions, the professionalization of the technology sector gradually marginalized women's roles within computing. As computing became associated with higher levels of prestige, economic power, and technical specialization, gender stereotypes increasingly shaped hiring practices and workplace cultures. Women's expertise was often undervalued, and many were discouraged from pursuing long-term careers in

⁸⁹ Singer PW and Friedman A, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014)

⁹⁰ Brenner SW, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press 2012)

⁹¹ Ibid.

⁹² Deibert R, *Black Code: Surveillance, Privacy and the Dark Side of the Internet* (Signal Books 2013)

science and technology. Over time, this shift contributed to the gender imbalance that continues to characterize the technology sector today. The cybersecurity industry, in particular, remains heavily male-dominated. Global estimates suggest that women constitute only a small proportion of the cybersecurity workforce. Although this figure has gradually increased over time, the gender gap remains substantial.

The limited representation of women within cybersecurity has important consequences for the development of digital security frameworks. Diversity within technological fields is crucial for addressing complex challenges, as different perspectives and experiences contribute to more comprehensive solutions. When women are underrepresented in decision-making roles, the specific vulnerabilities they face may remain overlooked within policy and technological design. The absence of female role models and mentors also discourages younger generations of women from pursuing careers in cybersecurity, perpetuating a cycle of underrepresentation. At the same time, the expansion of digital platforms has intensified various forms of cyber violence directed at women.⁹³ Online harassment, misogynistic abuse, and targeted hate campaigns have become increasingly visible in social media environments. Surveys conducted in different regions suggest that a significant proportion of women have experienced some form of online harassment. Female journalists, activists, academics, and public figures often face coordinated digital attacks designed to silence their voices and discourage participation in public debate.

Cyberstalking represents another significant dimension of gendered cyber insecurity. This form of abuse involves persistent monitoring or harassment through digital technologies, including unauthorized access to personal accounts, spyware installations, and location tracking through GPS-enabled devices. In many cases, cyberstalking occurs within intimate relationships, where abusive partners use technology as a tool of control. Digital surveillance can restrict victims' autonomy, undermine their sense of safety, and escalate into real-world threats. Non-consensual dissemination of intimate images has also emerged as a pervasive form of cyber violence. The unauthorized sharing of private photographs or videos—often referred to as revenge pornography—can have devastating consequences for victims. Women subjected to such violations frequently experience emotional trauma, social stigma, and reputational damage. In certain contexts, victims may face exclusion from professional or social networks, and in extreme cases they may even encounter rejection from their own families. Despite the severity of these harms, legal frameworks in many jurisdictions remain inadequate for addressing such offences effectively. Another increasingly prevalent practice is doxxing, which involves the public release of personal information such as home addresses, contact details, or workplace information without consent. By exposing victims' private data, perpetrators create conditions that facilitate harassment, intimidation, and physical threats. Women who advocate for gender rights or challenge patriarchal norms are particularly vulnerable to such attacks, which are often intended to silence dissent and discourage activism.

⁹³ Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

These patterns of abuse reveal how patriarchal norms and gender biases are reproduced within digital environments. Online misogyny often reflects broader cultural attitudes that seek to police women's behaviour and restrict their participation in public spaces. The normalization of such behaviour within digital cultures can discourage victims from reporting abuse, particularly when institutional responses are slow or ineffective. The consequences of cyber violence extend beyond immediate emotional harm. Persistent harassment can affect women's professional opportunities, economic independence, and willingness to engage in digital platforms that are increasingly essential for career development. Female entrepreneurs, journalists, and professionals often rely on digital tools for networking, communication, and business promotion. However, exposure to cyber harassment, identity theft, or privacy violations may discourage them from maintaining an active online presence. Women in developing regions face additional vulnerabilities due to limited access to technological resources and cybersecurity awareness. Structural inequalities in education, income, and digital infrastructure often restrict women's ability to benefit from technological advancements while simultaneously increasing their exposure to cyber risks. In such contexts, the digital divide intersects with gender inequality, reinforcing patterns of marginalization.⁹⁴ These dynamics highlight the importance of examining cybersecurity not only as a technological challenge but also as a social phenomenon shaped by power relations, institutional structures, and cultural norms. Understanding the gendered dimensions of cyber insecurity requires a broader analytical framework that situates digital threats within the context of structural inequality and social transformation. Such an approach opens the way for deeper exploration of how online violence operates, how institutional responses have evolved, and how gender-sensitive cybersecurity frameworks can be developed to address these emerging challenges in the contemporary digital era.⁹⁵

Cybersecurity Governance and the Evolving Landscape of Global Digital Threats

The rapid digitalization of contemporary societies has transformed data, digital infrastructures, and interconnected networks into central components of economic activity, governance, and everyday life. As organizations, governments, and individuals increasingly rely on complex technological systems to conduct operations, the importance of cybersecurity governance has grown substantially.⁹⁶ Cybersecurity governance broadly refers to the institutional frameworks, policies, and decision-making processes through which organizations manage cyber risks, protect digital assets, and ensure compliance with legal and regulatory standards. It functions as the strategic backbone of cybersecurity management by establishing accountability structures, clarifying responsibilities, and aligning security practices with broader organizational objectives. In an era characterized by accelerating digital transformation, cybersecurity governance has become indispensable for maintaining operational continuity, safeguarding sensitive information, and strengthening resilience against increasingly sophisticated cyber threats. At its core, cybersecurity governance provides a systematic approach to identifying, assessing, and mitigating cyber risks. It encompasses the development of policies, oversight mechanisms, and risk management strategies

⁹⁴ Floridi L, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford University Press 2014)

⁹⁵ Ibid.

⁹⁶ MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012)

that enable organizations to protect their digital infrastructure and respond effectively to emerging threats. Without effective governance structures, cybersecurity initiatives often remain fragmented, leaving critical gaps that can be exploited by malicious actors. By defining clear roles and responsibilities and integrating cybersecurity into broader organizational strategies, governance frameworks enable institutions to adopt proactive rather than reactive approaches to digital risk management. In doing so, they help organizations anticipate vulnerabilities, strengthen defence mechanisms, and ensure that cybersecurity remains aligned with institutional priorities and regulatory requirements.

The significance of cybersecurity governance has become more pronounced as the digital landscape continues to expand in scale and complexity. The increasing reliance on interconnected systems, cloud-based services, and digital platforms has created a highly integrated technological ecosystem in which vulnerabilities in one component can rapidly cascade across multiple networks. In such an environment, cyberattacks can have far-reaching consequences, affecting not only individual organizations but also entire industries and national infrastructures. Effective governance frameworks therefore play a crucial role in coordinating security strategies, ensuring regulatory compliance, and fostering collaboration among stakeholders responsible for protecting digital systems.⁹⁷ One of the primary functions of cybersecurity governance is to address the growing risks associated with cybercrime and data privacy violations. The absence of coherent governance structures often results in inconsistent security policies and inadequate risk management practices, creating opportunities for cybercriminals to exploit weaknesses in digital systems. By establishing standardized procedures for risk assessment, incident response, and compliance monitoring, governance frameworks help organizations minimize exposure to cyber threats while maintaining transparency and accountability. Furthermore, effective governance strengthens trust between organizations and their stakeholders by demonstrating a commitment to safeguarding sensitive information and protecting user privacy.⁶⁹ The expanding digital ecosystem has simultaneously intensified concerns regarding the protection of personal and organizational data. Data has become one of the most valuable assets in the modern economy, driving innovation, enabling personalized services, and facilitating strategic decision-making. However, the increasing volume and sensitivity of data collected by institutions also amplify the risks associated with unauthorized access, misuse, and breaches. Data protection has therefore emerged as a central concern within cybersecurity governance, requiring robust frameworks capable of balancing security, privacy, and technological innovation.⁷⁰

The contemporary cybersecurity landscape is marked by a growing number of sophisticated and large-scale cyber incidents that reveal the vulnerabilities inherent in interconnected digital infrastructures. High-profile attacks in recent years have underscored the systemic risks associated with weak cybersecurity governance. Incidents such as the SolarWinds supply chain breach and the ransomware attack on the Colonial Pipeline illustrate how cyber threats can disrupt critical infrastructure, compromise sensitive information, and inflict substantial financial and reputational

⁹⁷ MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012)

⁶⁹ Deibert R, *Black Code: Surveillance, Privacy and the Dark Side of the Internet* (Signal Books 2013) ⁷⁰ Ibid.

damage.⁹⁸ These attacks not only exposed weaknesses in organizational security practices but also highlighted the broader implications of cyber vulnerabilities for national economies and public trust in digital systems. The economic consequences of cybercrime are particularly striking. Global estimates indicate that cybercrime imposes trillions of dollars in annual losses on the global economy, with projections suggesting that these costs will continue to rise as digitalization expands. Financial losses associated with cyberattacks include direct theft, ransom payments, operational disruptions, and the costs of recovery and remediation. However, the implications of cyber incidents extend far beyond immediate financial damage.⁹⁹ Data breaches and service disruptions can undermine public confidence in digital technologies, discourage technological adoption, and hinder innovation within digital economies. Cyberattacks targeting essential services further illustrate the societal implications of inadequate cybersecurity governance. Attacks on healthcare systems, for instance, can disrupt medical services and jeopardize patient safety by disabling critical information systems. The ransomware attack on Ireland's Health Service Executive demonstrated how cyber incidents can interfere with healthcare delivery, forcing hospitals to cancel procedures and delay treatments. Such incidents highlight the vulnerability of critical infrastructure sectors that rely heavily on digital systems for operational efficiency and service provision.¹⁰⁰

Beyond economic and societal impacts, cybersecurity governance has also become a matter of national security. State-sponsored cyber operations have increasingly targeted government institutions, defence systems, and electoral processes, raising concerns about the use of cyberspace as a domain of geopolitical competition. Cyberattacks directed at energy infrastructure, communication networks, and financial systems can destabilize entire regions by disrupting essential services and undermining public confidence in national institutions. The coordinated cyberattacks on Ukraine's power grid during the mid-2010s demonstrated how cyber warfare can directly affect critical infrastructure, leaving millions without electricity and highlighting the strategic potential of cyber operations in modern conflicts.¹⁰¹ Within this evolving threat landscape, cybercrime itself has become increasingly sophisticated and diversified. Among the most prevalent forms of cyber threats are ransomware attacks, phishing campaigns, and supply chain compromises, each exploiting different vulnerabilities within digital ecosystems. Ransomware attacks have expanded dramatically in scale and complexity, targeting organizations across sectors ranging from healthcare and education to energy and finance. These attacks involve malicious software that encrypts a victim's data and demands payment for its release. The global impact of ransomware was dramatically illustrated by the WannaCry attack in 2017, which affected hundreds of thousands of computer systems across multiple countries and disrupted critical services worldwide. In recent years, ransomware tactics have evolved to include "double

⁹⁸ Nissenbaum H, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press 2010)

⁹⁹ Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

¹⁰⁰ Ibid.

¹⁰¹ Greenberg A, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday 2019)

extortion,” where attackers not only encrypt data but also threaten to publicly release sensitive information if ransom demands are not met.

Phishing attacks remain another highly effective method used by cybercriminals to infiltrate organizational networks. These attacks exploit human vulnerabilities rather than technical weaknesses, manipulating individuals into revealing confidential information such as login credentials or financial details. The increasing sophistication of phishing techniques—including spear phishing and business email compromise schemes—has made detection and prevention more challenging for organizations. Because phishing often relies on deception rather than technical intrusion, addressing such threats requires a combination of technological safeguards and user awareness initiatives. Supply chain attacks have emerged as particularly concerning threats within interconnected digital ecosystems. By targeting third-party vendors or service providers, attackers can infiltrate otherwise secure organizations and gain access to sensitive networks. The SolarWinds breach represents a striking example of how vulnerabilities within supply chains can be exploited to compromise thousands of organizations simultaneously, including government agencies and major corporations.¹⁰² Such incidents illustrate how the interconnected nature of modern digital infrastructures creates systemic risks that extend far beyond individual institutions. Advanced persistent threats and state-sponsored cyber operations represent another dimension of contemporary cyber risk. These threats are typically characterized by long-term, stealthy infiltration of targeted systems, often aimed at extracting valuable intelligence or compromising strategic assets. Operations such as the Stuxnet attack on Iranian nuclear facilities demonstrated the potential of cyber tools to achieve strategic objectives traditionally associated with conventional military operations. Similarly, various state-linked hacking groups have been accused of conducting prolonged campaigns targeting intellectual property, industrial secrets, and government communications across multiple countries. Alongside these threats, the challenges of protecting data privacy have become increasingly complex. Data breaches have become a recurring feature of the digital age, exposing sensitive personal information such as financial records, health data, and identification details. Large-scale breaches affecting social media platforms and technology companies have demonstrated how vulnerabilities in data protection practices can expose millions of users to identity theft, fraud, and other forms of exploitation. Beyond the immediate consequences for affected individuals, such incidents also erode public trust in digital platforms and raise questions about the ethical responsibilities of organizations that collect and store vast amounts of personal data. Concerns about surveillance further complicate the relationship between cybersecurity governance and data privacy. Governments often justify extensive surveillance programs as necessary for national security and law enforcement purposes. However, these initiatives frequently raise concerns about the balance between security and individual privacy rights. Revelations regarding mass surveillance activities have intensified debates about the limits of governmental authority and the potential misuse of digital monitoring technologies. Similarly, corporate data collection practices—particularly those used for targeted

¹⁰² Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013) ⁷⁶ Ibid.

advertising and behavioural profiling—have raised ethical questions about consent, transparency, and the commercialization of personal information.¹⁰³

The issue of informed consent is particularly significant in the context of digital data governance. Many users unknowingly agree to extensive data collection practices through complex terms of service agreements that are rarely read or fully understood. High-profile controversies involving the misuse of personal data for political or commercial purposes have highlighted the consequences of weak consent mechanisms and inadequate oversight. These developments have prompted policymakers in several jurisdictions to introduce regulatory frameworks aimed at strengthening data protection and empowering individuals with greater control over their information. Among the most influential regulatory initiatives are the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These frameworks have sought to enhance privacy protections by establishing stricter requirements for data collection, processing, and storage. The GDPR, in particular, has established a global benchmark for data governance by emphasizing principles such as user consent, data minimization, and the right to erasure. Its extraterritorial application has compelled organizations around the world to adopt stronger data protection measures when handling information belonging to European citizens. Similarly, the CCPA has expanded consumer rights in the United States by granting individuals greater control over how their personal data is accessed and used by corporations.¹⁰⁴ Despite these advances, the global cybersecurity governance landscape remains fragmented and uneven. One of the most significant challenges arises from the cross-border nature of cybercrime. Cyberattacks frequently involve perpetrators, victims, and digital infrastructures located in different jurisdictions, complicating efforts to investigate and prosecute offenders. Jurisdictional boundaries, differences in legal definitions of cybercrime, and the absence of harmonized regulatory frameworks often allow cybercriminals to exploit gaps in international enforcement mechanisms. Attacks such as the global spread of the NotPetya malware demonstrated how cyber incidents can affect organizations across dozens of countries while remaining difficult to attribute or prosecute effectively.

International cooperation initiatives have attempted to address these challenges by promoting collaborative approaches to cybersecurity governance. Agreements such as the Budapest Convention on Cybercrime provide frameworks for information sharing and coordinated law enforcement efforts. However, the effectiveness of such initiatives is limited by uneven participation and differing national priorities. Several major countries have not ratified these agreements, citing concerns about sovereignty and fairness in the development of international legal frameworks. As a result, global efforts to combat cybercrime remain constrained by geopolitical tensions and disparities in technological capabilities among nations. Emerging technologies such as artificial intelligence and the Internet of Things further complicate the governance landscape.¹⁰⁵ AI systems rely on large volumes of data to function effectively, raising

¹⁰³ Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

¹⁰⁴ Rid T, *Cyber War Will Not Take Place* (Oxford University Press 2013)

¹⁰⁵ Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

concerns about transparency, bias, and accountability in automated decision-making processes. Meanwhile, the proliferation of IoT devices from smart home appliances to industrial sensors has introduced new vulnerabilities into digital networks. Many IoT devices are produced with minimal security features, making them attractive targets for cybercriminals seeking to exploit weaknesses in distributed networks. Incidents such as the Mirai botnet attack demonstrated how insecure IoT devices can be harnessed to launch large-scale distributed denial-of-service attacks capable of disrupting major internet services. These developments reveal significant gaps in existing cybersecurity governance frameworks. Many current policies focus primarily on reactive measures such as breach notifications and penalties rather than proactive strategies aimed at building resilience and preventing attacks. Small and medium-sized enterprises, in particular, often lack the resources required to implement comprehensive cybersecurity programs, creating vulnerabilities that can be exploited by attackers. At the same time, regulatory fragmentation across jurisdictions continues to complicate compliance efforts for organizations operating in global digital markets.¹⁰⁶

The growing nuances of cyber threats, the rapid evolution of digital technologies, and the persistent fragmentation of governance frameworks collectively underscore the need for more adaptive and coordinated approaches to cybersecurity governance. Addressing these challenges requires not only stronger regulatory frameworks but also greater international cooperation, improved technological safeguards, and sustained investment in capacity-building initiatives. Within this evolving context, a deeper examination of governance mechanisms, policy frameworks, and institutional responses becomes essential for understanding how digital security can be strengthened in an increasingly interconnected world. Cybercrime against women has increasingly emerged as a significant concern within global governance frameworks, particularly within the institutional architecture of the United Nations. As digital technologies expand across societies, the risks associated with cybercrime, online harassment, and digital exploitation have grown in scale and complexity. Women, in particular, experience disproportionate exposure to cyber threats due to existing social inequalities, gender-based discrimination, and structural barriers that shape their access to digital spaces. International organizations have therefore begun to recognize the gendered dimensions of cybersecurity and the urgent need to develop institutional responses that address online violence, digital exclusion, and technological vulnerabilities affecting women.

International and National Responses to Cybercrime Against Women

Within the United Nations system, the International Telecommunication Union (ITU) has played a pivotal role in addressing evolving technological risks. Established in 1865, the ITU is one of the oldest international organizations and has historically been responsible for coordinating global telecommunication standards and policies. Over time, its mandate has expanded to encompass broader issues related to digital governance and cybersecurity. As communication technologies evolved from telegraph networks to the contemporary internet-based ecosystem, the ITU increasingly acknowledged that cybersecurity is a foundational component of a safe and connected global society. The proliferation of malware, cyber espionage, cyber terrorism, and organized

¹⁰⁶ Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

digital crime has intensified concerns about the security of digital infrastructures. These developments have not only affected governments and institutions but have also created new vulnerabilities for individuals navigating online environments. Women are often disproportionately affected by such threats, particularly in the form of cyber harassment, identity theft, online stalking, and the non-consensual dissemination of personal content. Complementing the technological focus of the ITU, the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), established in 2010, has played a central role in addressing the gendered implications of digital insecurity. UN Women operates as the primary United Nations body dedicated to advancing gender equality, promoting women's rights, and supporting global efforts to eliminate violence against women. The organization also engages with issues affecting marginalized communities, including violence against LGBTQ+ individuals and gender minorities, particularly within digital spaces. Through its governance structure—

comprising an executive board representing different geographic regions—UN Women operates within the broader framework of the United Nations Charter to promote inclusive policies and gender-responsive strategies. In recent years, the organization has expanded its focus to include the intersection between gender, peace, and cybersecurity. Recognizing the growing role of digital technologies in shaping social and political life, UN Women initiated the “Women, Peace and Cybersecurity” project in 2021, aimed at enhancing women's participation in cybersecurity governance and promoting safer digital environments. Such initiatives reflect a broader acknowledgment that cybersecurity must incorporate gender-sensitive perspectives in order to address the distinct challenges faced by women in digital spaces. In 2024, UN Women further strengthened these efforts by launching a free e-learning platform designed to equip women with knowledge and practical skills relevant to the digital age. By providing accessible training resources, the initiative seeks to bridge the digital literacy gap and empower women to navigate technological environments with greater confidence and security. Alongside international efforts, national governments have also begun developing legal frameworks to address cybercrime against women.

In India, the rise in cyber offenses targeting women has prompted the development of a multilayered legislative architecture aimed at regulating digital conduct and protecting victims. The Information Technology Act, 2000 constitutes the primary legal instrument governing cyber offenses in India. It criminalizes activities such as hacking, identity theft, unauthorized access to digital systems, and electronic stalking. The Act also provides for the establishment of specialized cybercrime investigation cells that are tasked with addressing digital offenses more effectively. In addition to the IT Act, provisions within the Indian Penal Code (IPC) have been amended to address emerging forms of cyber-enabled violence. Legal provisions now cover offenses such as voyeurism, cyberstalking, and the non-consensual dissemination of intimate images, commonly referred to as “revenge pornography.”¹⁰⁷ The Protection of Women from Domestic Violence Act, 2005 further extends protection to cases where digital technologies are used within abusive relationships to harass, threaten, or monitor victims. These legal instruments collectively reflect an

¹⁰⁷ Crete-Nishihata M and Deibert R (eds), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (MIT Press 2012)

effort to adapt existing criminal justice frameworks to the realities of the digital era. Despite the existence of this normative legal structure, challenges related to enforcement, institutional capacity, and public awareness continue to limit its effectiveness. Many victims remain unaware of the legal protections available to them, while law enforcement agencies often face resource constraints and technical limitations when investigating cyber offenses. The gap between legislative provisions and their implementation therefore remains a significant obstacle to ensuring meaningful digital protection for women. Statistical trends further highlight the growing scale of the problem. Reports indicate that cybercrimes against women in India have increased steadily in recent years. In 2022 alone, the National Commission for Women reportedly received over 31,000 complaints related to crimes against women, including online harassment and digital abuse. Among these offenses, the non-consensual circulation of intimate images—commonly described as revenge pornography—has become one of the most disturbing manifestations of cyber violence. Such crimes not only violate personal privacy but also expose victims to severe psychological distress, social stigma, and reputational harm.

Indian law contains several provisions intended to address these forms of digital abuse. Section 72 of the Information Technology Act, 2000 criminalizes the unauthorized disclosure of personal information obtained through digital means. Any individual who discloses or publishes such information without consent may face imprisonment of up to three years, a monetary fine that may extend to five lakh rupees, or both. The provision emphasizes the protection of individual privacy and recognizes the harm caused by the misuse of personal data. The constitutional dimension of privacy protection was further strengthened in 2017 when the Supreme Court of India delivered its landmark judgment in *Justice K.S. Puttaswamy v. Union of India*. In this historic ruling, a nine-judge constitutional bench affirmed that the right to privacy is a fundamental right under Article 21 of the Constitution, which guarantees the right to life and personal liberty.¹⁰⁸ The judgment marked a transformative moment in Indian constitutional jurisprudence by recognizing privacy as an essential component of human dignity and autonomy in the digital age. However, despite these legal and constitutional advancements, the persistence of cybercrime across Indian states illustrates the continuing challenges of translating legal protections into effective safeguards. Rapid digitalization, uneven access to cybersecurity awareness, and persistent gender inequalities contribute to an environment in which women remain vulnerable to online abuse. Consequently, addressing cybercrime against women requires not only stronger enforcement mechanisms but also sustained institutional efforts to enhance digital literacy, strengthen investigative capacity, and promote gender-sensitive approaches within cybersecurity governance.¹⁰⁹

Conclusion

Despite the existence of an extensive statutory and institutional framework addressing cybercrime against women, the practical effectiveness of these mechanisms remains subject to critical scrutiny.

¹⁰⁸ Zuboff S, *The Age of Surveillance Capitalism* (PublicAffairs 2019)

¹⁰⁹ Brown I and Marsden C, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013)

The present analysis suggests that a significant gap persists between the normative strength of legal provisions and their operational implementation. India possesses a layered legal architecture that includes the Information Technology Act, 2000, relevant provisions of the Indian Penal Code, and specialized statutes such as the Protection of Women from Domestic Violence Act, 2005 and the POCSO Act, 2012. In addition, constitutional jurisprudence has reinforced the importance of privacy and dignity through the recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017). Together, these instruments create a comprehensive legal framework that formally recognizes the seriousness of cyber violence and the need to safeguard women in digital spaces. However, the persistence and growing visibility of cyber offences indicate that the existence of legal protections alone does not necessarily translate into effective prevention or redress.

A closer examination reveals that the disparity between “law on the books” and “law in action” remains a defining challenge within India’s cybersecurity governance framework. While legislative provisions criminalize acts such as identity theft, cyberstalking, voyeurism, and the non-consensual dissemination of intimate images, enforcement mechanisms often struggle to keep pace with the rapidly evolving nature of digital threats. Law enforcement agencies frequently encounter technical limitations, shortages of trained personnel, and jurisdictional complications when investigating cyber offences. The transnational nature of digital crimes further complicates prosecution, as perpetrators may operate across multiple jurisdictions while exploiting anonymity and technological sophistication. Consequently, victims often face procedural delays, difficulties in evidence collection, and limited institutional support, which collectively weaken the deterrent value of existing legal provisions. Statistical trends further underscore the complexity of the problem. Reported cases of cybercrime against women have increased steadily in recent years, reflecting a pattern that is simultaneously encouraging and concerning. On one hand, the rise in reported complaints may indicate growing awareness among women about their legal rights and greater willingness to approach institutional mechanisms such as the National Commission for Women or specialized cybercrime cells. On the other hand, the upward trajectory of these cases also suggests that cyber offences themselves are expanding in scale as digital technologies become more deeply embedded within everyday life. The proliferation of social media platforms, online financial services, remote work systems, and digital communication tools has transformed the internet into an indispensable infrastructure for modern living. In such a context, complete disengagement from digital environments is neither practical nor desirable. Women must participate in these spaces for education, employment, social interaction, and civic engagement. Yet this very participation simultaneously increases their visibility and accessibility within digital networks, often exposing them to new forms of vulnerability and exploitation.

This structural dependence on digital systems therefore creates a paradoxical condition. While digital technologies offer unprecedented opportunities for empowerment, connectivity, and economic participation, they also expand the terrain on which gender-based violence can occur. Cyber harassment, stalking, doxxing, and non-consensual image dissemination illustrate how traditional forms of gendered violence have migrated into digital environments, often amplified by the speed, anonymity, and reach of online platforms. Addressing these challenges requires moving beyond a narrow focus on statutory adequacy toward a broader examination of institutional readiness and governance capacity. It is essential to assess whether law enforcement agencies possess the technological infrastructure, investigative expertise, and gender-sensitive protocols

necessary to respond effectively to cyber offences. Equally important is the question of accountability. Violations may originate not only from individual offenders but also from systemic failures within institutions, regulatory frameworks, or digital platforms themselves. In such cases, the assumption of the state as an unequivocal protective actor becomes more complex and warrants careful scrutiny. Against this background, the chapter highlights the need for a multidimensional approach to cybersecurity governance that integrates legal, technological, and social perspectives. Ensuring meaningful digital safety for women requires sustained investment in institutional capacity-building, specialized cybercrime training for law enforcement agencies, and stronger coordination between regulatory bodies, technology companies, and civil society organizations. At the same time, initiatives aimed at strengthening digital literacy and cybersecurity awareness among women remain crucial for enabling individuals to recognize and respond to online threats.

Ultimately, it suggests that cybersecurity frameworks often function reactively rather than preventively. Regulatory mechanisms frequently emerge in response to technological disruptions rather than anticipating them. As digital innovation continues to accelerate, the gap between technological capability and regulatory adaptation may widen further unless proactive governance strategies are adopted. Evaluating the effectiveness of cybersecurity frameworks therefore requires asking whether they operate as genuine deterrents capable of preventing cyber offences or whether they primarily function as post-facto response systems activated only after harm has already occurred. This question forms a critical foundation for the subsequent analysis undertaken in this study, which seeks to examine how legal institutions, governance mechanisms, and technological systems can be strengthened to ensure that women's digital safety becomes a substantive reality rather than a merely aspirational promise in an increasingly technologized society.
